

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 089 516 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

04.04.2001 Bulletin 2001/14

(51) Int. Cl.⁷: **H04L 29/06, G06F 1/00**

(21) Application number: **00203266.2**

(22) Date of filing: **20.09.2000**

(84) Designated Contracting States:

**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**

Designated Extension States:

AL LT LV MK RO SI

(30) Priority: **24.09.1999 US 155853 P**

(71) Applicant:

**Citicorp Development Center, Inc.
Los Angeles, California 90066 (US)**

(72) Inventors:

- **Grandcolas, Michael L.
Santa Monica, CA 90405 (US)**
- **Law, France
Los Angeles, CA 90034 (US)**

• **Doshi, Ashwin**

Cerritos, CA 90703 (US)

• **Williams, Michael**

Thousand Oaks, CA 91362 (US)

• **Jang, Yeona**

Princeton, NJ 08540 (US)

• **Merschen, Toni**

White Plains, NY 10605 (US)

• **Pan, Jack**

Rowland Heights, CA 91748 (US)

(74) Representative: **Hynell, Magnus**

Hynell Patenttjänst AB,

Patron Carls väg 2

683 40 Hagfors/Uddeholm (SE)

(54) **Method and system for single sign-on user access to multiple web servers**

(57) Methods and systems for single sign-on user access to multiple web servers are provided. A user is authenticated at a first web server (e.g., by user name and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a second web server offering the service indicated by the selector). When the user activates the service selector, the first web server constructs and transmits an encrypted authentication token (e.g., a cookie) from the first web server to a second web server via the user client. The first and second web servers share a sub-domain. The authentication token comprises an expiration time and is digitally signed by the first web server and is authenticated at the second web server. Upon authentication, the second web server allows the user to conduct a session at the second web server.

EP 1 089 516 A2

Description

I. Cross Reference to Related Application

- 5 [0001] This patent application claims priority to co-pending United States Provisional Patent Application Serial No. 60/155,853, entitled "Method and System for Single Sign-On User Access to a Federation of Web Servers," filed September 24, 1999, which is hereby incorporated in full by reference.

II. Field of the Invention

- 10 [0002] The present invention relates generally to the field of electronic commerce. More particular, embodiments of the present invention relate generally to a method and system for providing single sign-on user access to multiple web servers.

15 III. Background of the Invention

- [0003] There are many situations in which an entity or group of entities, such as a global financial institution with banking, brokerage, and other aspects, wishes to combine the functional resources of different web application servers in order to aggregate functionality to the customers of the entity or group of entities. Such an entity or group of entities may wish to allow their customers access to such an aggregated functionality by signing on only once, by authenticating themselves once, and then being able to use different services which might be provided either by different servers of entities within the group of entities, or by servers of the group of entities and, for example, by servers of third party entities.

- 25 [0004] In this context, the entity or group of entities may wish to deliver to the customer, via a web browser, a set of services that are hosted by different web application servers. Such application servers may employ different platforms, such as a UNIX platform, an NT platform, or some other type of platform. The platform may have been constructed by different organizations within the group of entities, or the platform may have been provided by third-party providers. In any event, an essential problem is how to allow the customer to sign on once and then to redirect the customer to these different servers without requiring the customer to sign on each and every time he or she goes accesses a different server.

- 30 [0005] Conventional products attempting to address this problem are deficient, for example, both in terms of performance and cost. In some such products, it is necessary to return to a centralized resource. Other such products do not support crossing organizational boundaries or Internet domain boundaries. What is needed is a methods and system for single sign-on user access to multiple web servers, such as a federation of web servers sharing sub-domains, that overcome such disadvantages and that provide other advantages.

IV. Summary of the Invention

- 40 [0006] The present invention provides methods and systems for single sign-on user access to multiple web servers, such as a federation of web servers sharing sub-domains, are provided. In an embodiment, a user is authenticated at a first web server (e.g., by user name and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a second web server offering the service indicated by the selector). Upon activation of the selector by the user, the first web server constructs, digitally signs, and transmits an encrypted authentication token (e.g., a cookie) from the first web server to a second web server via the user client. URL encoding is employed to encrypt and sign the authentication token. The first and second web servers share a sub-domain. The authentication token comprises an expiration time. The authentication token is examined and authenticated at the second web server and URL decoding is employed. Upon authentication, and if the expiration time has not passed, the second web server allows the user to conduct a session at the second web server.

- 50 [0007] In another embodiment, a method for single sign-on user access to a federation of web servers, such as a first and second web server sharing a sub-domain, is provided. In an embodiment, the method comprises allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device, authenticating the user with user-provided authentication information, including at least a user identification, by the first web server, and allowing the user to conduct a session at the first web server. During the session, the first web server carries out the functions of prompting the user for selection of a functionality offered via at least a second web server, and receiving a selection by the user of the functionality offered via the second web server.

55 Upon receiving a selection, the first web server creates an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server, digitally signing (e.g., by public key encryption) the authentication token by the first web server. An embodiment further comprises qualifying the domain attribute of the

authentication token with the shared sub-domain name by the first web server, sending the digitally signed authentication token to the web browser of the computing device by the first web server, redirecting the web browser to the second web server by the first web server, and sending the authentication token to the second web server by the web browser. The second web server decrypts the authentication token, confirms a match with the digital signature of the first web server, checks the pre-defined expiry of the authentication token by the second web server, and allows the user to conduct a session with the second web server if within the pre-defined token expiry.

[0008] In another embodiment, a method of single sign-on for multiple web servers, comprising receiving log-in data from a user in a first server, providing the user with a service selector, receiving an indication that the user selected the service selector, constructing an authentication token comprising profile data associated with the user, encrypting and signing the authentication token, redirecting the user to a second server, transmitting the authentication token to the user, receiving the authentication token in the second server, verifying the authentication token in the second server, and allowing the user access to a service provided by the second server. In one such embodiment, the authentication token comprises a cookie and further comprises expiration time data.

[0009] It is a feature and advantage of the present invention to provide a method and system for single sign-on user access to a federation of web servers that allows users already authenticated on a web site, such as a financial institution's web site, to have access, for example, to a service provider's web site without having to be re-authenticated via provision of a valid name and password.

[0010] To achieve the stated and other features and advantages, an embodiment of the present invention provides a method and system which enables single sign-on access for a user to a federation of web servers that allows user authentication at an entity's web site server, selection of a service provider URL, and passage of an authentication token by the entity's web site server to a service provider's server that contains sufficient information to enable the service provider's server, for example, to recognize the user as a valid service provider user and to provide the user with customer specific information.

[0011] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following, or may be learned by practice of the invention.

V. Brief Description of Figures

[0012]

FIG. 1 shows an embodiment of a system according to the present invention.

FIG. 2 shows a flow diagram describing a process according to the present invention carried out in the system shown in FIG. 1.

FIG. 3 shows a visual depiction of web pages associated with web servers of the system shown in FIG. 1.

FIG. 4 shows a flow diagram describing an alternative process according to the present invention carried out in the system shown in FIG. 1.

VI. Detailed Description

[0013] FIG. 1 shows an embodiment of a system according to the present invention. A brokerage firm web server (BFWS) 30 includes a brokerage firm web site 32. The brokerage firm web server 30 (and likewise the brokerage firm web site 32) is in communication with the Internet 20. Likewise, a bank web server 40 includes a bank web site 42. The bank web server (BWS) 40 (and likewise the bank web site 42) is also in communication with the Internet 20. A customer 5 of both the brokerage firm and the bank is shown. The customer 5 has a user name and password to access both the brokerage firm web site 32 and the bank web site 42. The customer's personal computer 10 having a web browser such as Microsoft Internet Explorer or Netscape Navigator (a client) is in communication with the Internet 20 as well. The customer 5 uses the customer's personal computer and browser 10 to communicate with the web servers 30, 40 via the Internet. Herein, the term customer is used in many instances to indicate the client 10 as used by the customer. In addition to network communication facilities and other aspects, the brokerage firm web server 30 and the bank server 40 comprise programming to carry out the functions described herein.

[0014] FIG. 2 shows a flow diagram of steps carried out in the system shown in FIG. 1. The customer 10 points the customer's browser to the brokerage firm web site 32. The customer 10 logs into the brokerage firm web site 32 using the customer's correct user name (or user identification) and password for the brokerage firm web site 32, and is authenticated by the brokerage firm web server 30. Once the customer logs into the brokerage firm web site 32, the web site 32 presents the customer 10 with a welcome page from the web site 32. Once logged in, the customer 10 may examine the customer's brokerage account information, portfolio, investment information, and the like.

[0015] FIG. 3 shows a graphical depiction of the system shown in FIG. 1, including the welcome page 100 from the

brokerage firm web site 30 provided to the customer 10 once the customer logs in at the brokerage firm web site 30. The welcome page 100 shown in FIG. 3 includes a service selector in the form of a hyperlink shown as "bill payment" 102. The brokerage web site offers its customers the ability to pay bills.

[0016] Referring again to FIG. 2, the customer 10 requests bill payment 50 by clicking on the "bill payment" hyperlink 102. The brokerage firm web server 30 itself does not handle the process of bill payment, but the server 30 is programmed with the knowledge that the bank web server 40 handles such a process. The hyperlink 102 includes the URL of the bank web site 42. Upon detecting the request of bill payment, the brokerage firm server 30 builds an authentication token 52. An authentication token comprises an object (or data) that can be passed between cooperating servers. A function of an embodiment of an authentication token is to convey the necessary information from a primary (or first) server to a secondary (or second) server to allow the secondary server to skip the sign-on process that would otherwise be necessary and required. Once a primary server establishes a session for a user, a cooperating secondary server that receives a valid authentication token from the primary server can establish a session without having the user sign on again.

[0017] In the embodiment shown in FIG. 1, the brokerage firm web server 30 builds an authentication token (or access token) comprising user identification data (or profile data) and expiration time data (token expiry) 52. The profile data comprises user identification data comprising a customer identification number that uniquely identifies the user to the secondary server. In the shown embodiment, the token also include a list of accounts of the customer. Expiration time data comprises data reflecting the time after which the authentication token is invalid. In the embodiment shown, the time is in Greenwich Mean Time (GMT). In other embodiments, the time may be in Universal Time. Expiration time may be set by the primary server at any desired time, though in most embodiments the expiration time is a relatively short time, e.g., three to twenty minutes, from the time at which the authentication token is created. In the embodiment shown, the expiration time is set at fifteen minutes from the time the authentication token is created. Note that it is important for the servers exchanging such authentication tokens to maintain correct or synchronized clocks. The use of expiration time is used to create a single-use, perishable token.

[0018] In the embodiment shown, the authentication token built comprises a cookie with profile data of the customer 5 and an expiration time of fifteen minutes from the creation time of the token. Authentication tokens may also comprise URL strings or other data that may be passed between servers. The profile data of the customer includes a customer identification number for the customer 5. The brokerage firm web server 30 includes a data storage system (e.g., a hard disk drive) that has customer identification numbers associated with log-in user names used by customer's of the brokerage firm web server 30. These numbers were agreed upon previously by the administrators of the servers 30, 40. In the embodiment shown, a customer is associated with a customer identification number. In the embodiment, when the customer requests bill payment 50, the server 30 retrieves, from the data storage system, the customer identification number for the customer 5. This customer identification number retrieved is used in the profile data used to build the cookie 52.

[0019] In another embodiment, various customer identification numbers are associated with various secondary servers. When the customer requests a service provided at a secondary site (or to be transferred to a secondary site), the primary server detects the request, determines the secondary site, and retrieves, from the data storage system, the customer identification number for the requesting customer that is associated with the secondary site to which the customer will be directed for bill payment services.

[0020] Referring again to FIG. 2, the server 30 also selects the secondary server recipient name 54. The server 30 does so by examining the request made by the customer and determining the name / address of the appropriate secondary server to handle the request. In the embodiment shown, the server 30 examines the "bill payment" request made by the customer. In the present embodiment, the examination comprises determining the Uniform Resource Locator (URL) associated with the "bill payment" hyperlink. The web page file associated with the welcome page 100 includes the URL associated with the "bill payment" hyperlink, and the server 30 selects this URL.

[0021] The server 30 then signs and encrypts the cookie 56. A digital signature associated with the brokerage firm server 30 is applied to the cookie 56 by the server 30. Preferably, the server 30 comprises public key encryption software capable of encrypting, digitally signing, and authenticating electronic transactions across applications and servers. In the embodiment shown, the Entrust/PKI 5.0 software package, with its associated application programming interface (API) library, available from Entrust Technologies, Inc., Plano, Texas, is used to sign the cookie using a public key encryption system. In the embodiment shown, the cipher used is the Triple DES (Data Encryption Standard) encryption algorithm system, the encrypted cookie uses privacy-enhanced mail (PEM) headers, and signing uses the Secure Hash Algorithm (SHA-1) to create the message digest (or hash value) in signing. The Triple DES system is used to encrypt the authentication token (the cookie), and a PEM header and SHA-1 digest is included.

[0022] A digital signature associated with the server 30 (in the form of a signed-encrypted string) applied to the cookie allows a secondary server to verify that the authentication token was created by the brokerage firm server 30. Further, the signature allows a secondary server to detect any modification or corruption of the authentication token. The digital signature is applied and encrypted by the server 30.

[0023] In the embodiment shown, the cookie is created and kept on the browser 10 of the user 5 using a header entry in the response page, and the header entry is structured as follows: Set-cookie; name=value; expires=date-time; domain=domainname; path=path; secure. The path value comprises a specific directory, and the domainname value preferably is a common sub-domain (discussed further below). In an embodiment, the authentication token (the cookie) is non-persistent and will not be written to disk on the customer client 10. In such an embodiment, an expires value is not necessary, and the cookie will be deleted by the receiving server immediately after receipt.

[0024] An example of a string comprising cookie construction according to an embodiment of the present invention is as follows:

VER11EXPDT11999050513254011CT\CUSTIAFIEXIST11CID157600100056005023 411
FCID1011TAI211ANM100100000011RTN109911ANAMy wife's
Checking11ABI23760011ANM1001000000211RTN00911ANAMy
checking11ABI24556. The example is in the following format: Tag1 TagValue1 Tag2 TagValue2 Tag3 TagValue3

[0025] It is noted that the specific tags and their tag values may vary according to implementation needs, such as destination server requirements.

[0026] Tags in the example shown, their value, and a description is shown in the following table:

Tag	Tag Value	Description
VER	1	Version of cookie system being used (current version is 1)
EXPDT	Date / Time	The ASCII GMT date and time that the authentication token expires. Format: CCYYMMDDHHMMSS.
CT	CUST FC	Customer Type. CUST= regular customer. FC= Customer Representative. Used to activate view-only mode.
AF	NEW / EXIST	New or existing customer indicator.
CID	Integer	Customer Identification Number
FCID	Alphanumeric	Identification number for customer service representative. If the user is a regular customer, do not set FCID (i.e., set to 0).
TA	Integer	Total Number of Accounts of customer
ANM	Integer	Account Number
RTN	Integer	Routing transit Number - maps to prod-type-cd
ANA	Alphanumeric	Account nick name
AB	Integer	Account Balance in cents (i.e. \$10.50=1050)

[0027] In the embodiment shown, the order of tags is not significant, except for ANM, ANA, AB, which are considered a tuple and are grouped together as shown above. Also, in the embodiment shown, the VER, EXPDT, and CT are required tags. Other tags that may be used in other embodiments include the following: AG (agency or corporation name that employs the user), FNAM (first name of user), and LNAM (last name of user).

[0028] The AF tag allows the bank server 40 to determine if an "Activate User" message should be sent to a transaction processing system (TPS). Preferably, if the brokerage firm web server 30 cannot determine whether a customer is new or already enrolled with GTPS, the server 30 sets the AF tag to NEW. In addition, the brokerage firm web server 30 shown assumes that all accounts are of the "Checking" type, and will set the product type code based on the RTN value determined.

[0029] The brokerage firm server 30 then URL encodes (also called URLEncode) the constructed cookie 58. Essentially, in URL encoding the cookie, the broker firm web server converts the formatted string discussed above to a URL-encoded format. In one embodiment, the URL encoding encodes the string using the URL escape syntax which comprises a three character string (%nn) specifying the hexadecimal code for a character. This syntax is used to hide characters that may be otherwise significant when used in a URL. The URL encoding 58 carried out by the brokerage firm web server 30 results in an encoded, signed, and encrypted string suitable for writing in a cookie, and such string is included in the cookie built by the server 30.

[0030] The brokerage firm web server 30 then sends a redirect command (or redirect page) with the URL encoded cookie (the authentication token) in a set-cookie header to the customer client 60. The redirect command includes the URL of the web site associated with "bill payment" 42. The customer client 10 receives the redirect command and the URL encoded cookie constructed by the brokerage web server 30.

5 **[0031]** The customer client 10 connects with the bank web site 42 via the Internet 20 and sends the cookie to the bank web server 62. In the embodiment shown, the authentication token is transmitted in a Secure Sockets Layer (SSL) session. Further, in the embodiment shown, on receipt of the redirect command, the customer client 10 opens a second browser window, requests a download of the home page at the URL of the web site 42 (or the page designated in the URL), receives the page of the web site 42 from the bank web server 40, and displays the page in the window. An
10 embodiment of such a window 110 and page is shown in FIG. 3. The cookie received by the customer client 10 from the brokerage firm web server 30 is sent by the customer client 10 to the bank web server 40.

[0032] The bank web server 40 receives the cookie from the customer client 10. The bank web server 40 decodes the encoded, signed, and encrypted string built into the cookie by the brokerage firm web server 30 into a signed, encrypted string 64. Such decoding employs URL Decoding (or URLDecode) methods in the embodiment shown. In
15 the embodiment shown, URL Decoding is employed to convert the URL encoded string in the cookie to plain ASCII for examination by the bank web server 40. The bank web server 40 and the brokerage firm web server 30 previously exchanged public-private key decryption information.

[0033] Once the string is decoded, the bank web server 40 decrypts and verifies the cookie (including the signed, encrypted string that is now decoded) 66. In the embodiment shown, software comprising public key encryption software capable of decrypting and authenticating electronic transactions across applications and servers is used by the
20 bank web server 40 to do so. One example of such software is the Entrust/PKI 5.0 software package, with its associated application programming interface (API) library, available from Entrust Technologies, Inc., Plano, Texas.

[0034] The bank web server 40, using the software mentioned, determines whether the digital signature associated with the cookie verifies 68. If the signature does not verify, the bank web server 40 rejects the attempted sign-on and re-directs the customer client 10 to a web page on the brokerage firm web server 30 indicating an error and sign-on
25 failure 70, resulting in a failed sign-on attempt 72. In another embodiment, if the signature does not verify, the bank web server 40 rejects the sign-on and sends a web page indicating an error and sign-on failure to the customer client 10. In an embodiment, if the signature does not verify, the bank web server 40 also sends a message indicating such failure to the brokerage firm web site 30, e.g., an e-mail message.

30 **[0035]** If the signature verifies, the bank web server 40 examines the Certificate Authority (CA) name associated with the cookie 74. The server 40 compares the CA name associated with the cookie (i.e., the CA used with the CA name expected, as recorded in a registry file in the bank web server 40). If the CA name is not the one expected, the bank web server 40 re-directs the customer client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above.

35 **[0036]** If the CA name is the CA name expected, the bank web server 30 next if the sender's name is correct 76. In doing so, the bank web server 30 determines whether the Common Name (CN) associated with the cookie (i.e., the name being certified — the name used by the brokerage firm web server 30) is an authorized name. In so determining, the bank web server 40 compares the CN associated with the cookie with a file containing authorized names in a data registry in the bank web server 40. If the CN is not the one expected, the bank web server 40 re-directs the customer
40 client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above.

[0037] If the CN is correct, i.e., if the CN is an authorized name, the bank web server 40 extracts profile data from the cookie and begins a bill-payment session 78. In the embodiment shown, the server 40 parses the clear text data associated with the cookie (clear text refers to the information that is not encrypted) 78, and examines the expiration time data in the cookie (not shown). If the expiration time has passed, the bank web server 40 re-directs the customer
45 client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above. The clear text data includes profile data (e.g., customer identification number). If the expiration time has not passed, the web server 40 begins a bill payment session using the session and profile data 78 by sending the customer client the web page 110 of the bank web site 42 that is shown in FIG. 3, and the sign-on is successful 80. The customer client 10 receives the web page 100 and proceeds with the bill-payment session with the bank server 40. In an embodiment, the
50 authentication token (cookie) is then discarded or destroyed by the web server 40.

[0038] In an alternative embodiment, the system reflects a service associated with a user's employee. One such embodiment is shown in FIG. 4. In the embodiment shown in FIG. 4, the process of this alternative embodiment generally proceeds as that discussed above, with exceptions discussed below. The embodiment shown employs a primary server comprising a central web server having a central web site (not shown). The central web site comprises a web
55 site at which the customer client 10 may request various services by clicking a hyperlink.

[0039] Referring to FIG. 4, the customer 5 signs on to the central web site 49, and the process 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 174, continues in a manner like that described above in relation to steps 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 74 shown FIG. 3, with the central web server serving as the primary server (the brokerage

web server served as the primary web server in the embodiment shown in FIG. 2) until the step shown as item 77 occurs. The primary server includes the following, additional tags in the cookie: AG (agency or corporation name that employs the user), FNAME (first name of user), and LNAME (last name of user). The service provider referred to in FIG. 4 comprises the secondary server, and in the embodiment shown comprises the bank web server 40. After the bank web server 40 determines that the sender's CA is correct, the web server 40 determines whether the customer / user's employer has signed up with the service provider associated with the secondary server (the bank web server 40) 77. The bank web server 40 includes a database containing a list of employers who signed up with the service offered by the bank web server 40. The web server 40 compares the agency or corporation name in the AG tag with the list of employers. If the name in the AG tag is not on the list, the web server 40 re-directs the customer client 10 back to the central web site for an error URL 70.

[0040] If the name in the AG tag is on the list, the web server 40 continues the process by extracting profile data from the cookie and beginning a bill-payment session 78. After the bank web server 40 extracts profile data from the cookie and begins a bill-payment session 78, the server 40 examines a database (not shown) associated with the server 40 that includes data reflecting users who have previously signed up for or used the service provided by the server 40. If the user reflected by the cookie exists (i.e., has previously signed up for or used the service provided by the server 40), the web server 40 retrieves a default web page previously selected as the user's default page and sends the default web page to the customer client 83, and the customer client 10 then may proceed with a bill-payment session 80.

[0041] If the user reflected by the cookie does not exist (i.e., the database does not reflect that the user has previously signed up for or used the service provided by the server 40), the web server 40 creates a user identification using the tag information, including the AG, FNAME, and LNAME tag information, and stores the user identification in a database. The server 40 then retrieves a pre-designated default web page and transmits the web page to the customer client 83. The pre-designated default web page comprises a pre-designated web page for users associated with the agency / corporation indicated in the AG tag. The customer client 10 then may proceed with a bill-payment session 80.

[0042] In an embodiment, multiple secondary servers are used in an embodiment of the present invention. In still other embodiments, multiple primary servers are used. A group of one or more primary and one or more secondary servers sharing log-in and other information as described herein may be referred to as a "federation" of servers.

[0043] In the embodiments shown herein, a digital certificate generation software program is used to generate certificates. An example of such software is the Entrust Solo Version 4.0 software package, available from Entrust Technologies, Inc., Plano, Texas. Preferably, when multiple secondary servers are employed in an embodiment of the present invention, the secondary servers will use the same profile (a file comprising information needed by the certificate before the server can authenticate). Also, preferably, the CN name in the profile matches the generic host name of the secondary server.

[0044] In embodiments, multiple primary servers are employed. The primary servers may use the same profile on all hosts or each host may use a separate profile. Like the secondary servers, certificates are employed in each primary server.

[0045] In an embodiment, servers sharing information between themselves that are maintained by different organizations use a shared domain in common in order to ease the sharing of information. In such an embodiment, a sub-domain is established or designated as the common sub-domain, the domain attribute of the authentication token (e.g., the shared cookie) is designated as the common sub-domain, and a "Forward IP (Internet Protocol) Pointer" entry is added in the DNS name servers of the cooperating organizations.

[0046] For example, the primary server sets a cookie sub-domain of xxxx.yyyy.com (wherein yyyy.com comprises the domain name of the primary server). Using "tail matching," cookies may be shared with any host whose domain tail is "yyyy.com." When the server searches a cookie list on the user's computer for valid or useable cookies, the server compares the domain attributes of the cookie with the Internet domain name of the host. If there is a tail match, then the cookie will go through path matching to see if it should be sent. "Tail matching" means that domain attribute is matched against the tail of the fully qualified domain name of the host. For example, a domain attribute of "xxxx.com" would match host names "yyyy.xxxx.com" as well as "zzzz.yyyy.xxxx.com." For example, the primary server with which the user interacts has a domain name of qqqq.yyyy.com, and the secondary server has a domain name of ssss.rrrr.yyyy.com, may share cookies in such an embodiment. In an embodiment, the IP pointer in the domain name server associated with the primary server either (1) maps the secondary server domain (ssss.rrrr.yyyy.com) to a pre-designated IP address associated with the secondary server; or (2) delegate the zone "rrrr" to a DNS name server associated with the secondary server for resolution.

[0047] As discussed above, certain embodiments of the present invention employ URL Encode and URL Decode. The following is a code fragment written in Microsoft C++ 6.0 showing an example of the implementation of URL Encode by a server:

```

//
// URLEncode converts some characters to %xx format for sending
5 // in a URL or writing to a cookie
//
10 void URLEncode (BYTE* szDecoded, BYTE* szEncoded)
{
    BYTE* pszInPtr = szDecoded;
15     BYTE* pszOutPtr = szEncoded;
    BYTE inch;

20     while ((inch = *pszInPtr++) != '\0')
    {
25         if (    (inch < 32) ||    (inch > 127) ||
                (inch == '=') ||    (inch == '?') ||
30                (inch == '&') ||    (inch == '+') ||
                (inch == '%') ||    (inch == '-') ||
                (inch == ':') ||    (inch == ';') ||
35                (inch == ','))
        {
            *pszOutPtr++ = '%';
40            sprintf((char*)pszOutPtr, "%02x", inch);
            pszOutPtr += 2;
        }
45     else
        *pszOutPtr++ = inch;
50     }
    *pszOutPtr++ = '\0';
55 }

```

[0048] The following code fragment shows the implementation of URL-Decode by as server:


```
//  
// URLDecode converts characters in the %xx format back to their ascii  
5 values  
//  
10 void URLDecode (BYTE* szEncoded, BYTE* szDecoded)  
   {  
       BYTE* pszInPtr = szEncoded;  
       BYTE* pszOutPtr = szDecoded;  
       int    inch;  
20       while ((inch = *pszInPtr++) != '\0')
```

```

    {
        if (inch == '%')
            *pszOutPtr++ = (unHex(pszInPtr++) << 4) +
                           unHex(*pszInPtr++);
        else
            *pszOutPtr++ = inch;
    }
    *pszOutPtr++ = '\0';
}

int unHex (BYTE hexChar)
{
    if ((hexChar >= '0') && (hexChar <= '9'))
        return hexChar - '0';
    if ((hexChar >= 'a') && (hexChar <= 'f'))
        return hexChar - 'a' + 10;
    if ((hexChar >= 'A') && (hexChar <= 'F'))
        return hexChar - 'A' + 10;
    return 0;
}

```

[0049] Those of ordinary skill in the art will recognize that there are a variety of code fragments useful in carrying out such steps. Further, a variety of programming languages may be used.

[0050] Various embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be apparent to those skilled in the art without departing from the spirit and scope of the present invention.

Claims

1. A method of single sign-on user access to multiple web servers, comprising:

authenticating a user at a first web server;
 transmitting an encrypted authentication token from the first web server to a second web server, wherein the authentication token comprises an expiration time and is digitally signed by the first web server;
 authenticating the authentication token at the second web server; and
 allowing the user to conduct a session at the second web server.

2. The method of claim 1 wherein the first web server and the second web server share a sub-domain.

3. The method of claim 2 further comprising examining the expiration time of the authentication token at the second

web server and allowing the user to conduct a session at the second web server only if the expiration time has not passed.

4. The method of claim 3 wherein the authentication token comprises a cookie.

5. The method of claim 4 wherein transmitting the encrypted authentication token from the first web server to the second web server comprises transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

6. The method of claim 5 wherein authenticating the user at the first web server comprises receiving a user name and password.

7. The method of claim 6 wherein transmitting the encrypted authentication token from the first web server to a second web server comprises transmitting the authentication token from the first web server to a computer of the user; and transmitting the authentication token from the computer of the user to the second web server.

8. The method of claim 7 wherein the first web server and the second web server comprise a federation of web servers.

9. The method of claim 8 wherein authenticating the authentication token at the second web server comprises examining the cookie.

10. The method of claim 9 further comprising URL encoding the authentication token.

11. The method of claim 10 further comprising URL decoding the authentication token at the second web server.

12. The method of claim 11 further comprising providing a web page to the user having a service selector.

13. The method of claim 12 wherein the service selector comprises a hyperlink.

14. The method of claim 13 wherein the hyperlink comprises a URL for the second web server.

15. A method for single sign-on user access to a federation of web servers, comprising:

allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device;
 authenticating the user with user-provided authentication information, including at least a user identification, by the first web server;
 prompting the user for selection of a functionality offered via at least a second web server;
 receiving a selection by the user of the functionality offered via the second web server;
 creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server;
 digitally signing the authentication token by the first web server;
 qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server;
 sending the digitally signed authentication token to the web browser of the computing device by the first web server;
 redirecting the web browser to the second web server by the first web server;
 sending the authentication token to the second web server by the web browser;
 decrypting the authentication token by the second web server;
 checking the pre-defined expiry of the authentication token by the second web server; and
 allowing the user to conduct a session with the second web server if within the pre-defined token expiry.

16. The method of claim 15 further comprising allowing the user to conduct a session with the first web server.

17. The method of claim 16 wherein the second web server shares a sub-domain with the first web server.

18. The method of claim 17 wherein digitally signing the authentication token by the first web server comprising digitally

signing the authentication token using public key encryption.

19. The method of claim 18 further comprising confirming a match with the digital signature.

5 20. A method of single sign-on for multiple web servers, comprising:

receiving log-in data from a user in a first server;
providing the user with a service selector;
receiving an indication that the user selected the service selector;
10 constructing an authentication token comprising profile data associated with the user;
encrypting and signing the authentication token;
redirecting the user to a second server;
transmitting the authentication token to the user;
receiving the authentication token in the second server;
15 verifying the authentication token in the second server; and
allowing the user access to a service provided by the second server.

21. The method of claim 20 wherein the authentication token further comprises expiration time data.

20 22. The method of claim 21 wherein the authentication token comprises a cookie.

23. The method of claim 22 wherein the log-in data comprises a user name and password.

24. The method of claim 23 wherein the service selector comprises a hyperlink.

25 25. A system for single sign-on user access to multiple web servers, comprising:

a means for authenticating a user at a first web server;
a means for transmitting an encrypted authentication token from the first web server to a second web server,
30 wherein the authentication token comprises an expiration time and is digitally signed by the first web server;
a means for authenticating the authentication token at the second web server; and
a means for allowing the user to conduct a session at the second web server.

35 26. The system of claim 25 wherein the first web server and the second web server share a sub-domain.

27. The system of claim 26 further comprising a means for examining the expiration time of the authentication token at the second web server.

40 28. The system of claim 27 wherein the authentication token comprises a cookie.

29. The system of claim 28 wherein the means for transmitting the encrypted authentication token from the first web server to the second web server comprises means for transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

45 30. The system of claim 29 wherein the means for authenticating the user at the first web server comprises means for receiving a user name and password.

31. The system of claim 30 wherein the means for transmitting the encrypted authentication token from the first web server to a second web server comprises means for transmitting the authentication token from the first web server to a computer of the user and means for transmitting the authentication token from the computer of the user to the second web server.
50

32. The system of claim 31 wherein the first web server and the second web server comprise a federation of web servers.
55

33. The system of claim 32 wherein the means for authenticating the authentication token at the second web server comprises means for examining the cookie.

34. The system of claim 33 further comprising a means for URL encoding the authentication token.

35. The system of claim 34 further comprising a means for URL decoding the authentication token at the second web server.

36. The system of claim 35 further comprising a means for providing a web page to the user having a service selector.

37. The system of claim 36 wherein the service selector comprises a hyperlink.

38. The system of claim 37 wherein the hyperlink comprises a URL for the second web server.

39. A system for single sign-on user access to a federation of web servers, comprising:

a means for allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device;

a means for authenticating the user with user-provided authentication information, including at least a user identification, by the first web server;

a means for prompting the user for selection of a functionality offered via at least a second web server;

a means for receiving a selection by the user of the functionality offered via the second web server;

a means for creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server;

a means for digitally signing the authentication token by the first web server;

a means for qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server;

a means for sending the digitally signed authentication token to the web browser of the computing device by the first web server;

a means for redirecting the web browser to the second web server by the first web server;

a means for sending the authentication token to the second web server by the web browser;

a means for decrypting the authentication token by the second web server;

a means for checking the pre-defined expiry of the authentication token by the second web server; and

a means for allowing the user to conduct a session with the second web server if within the pre-defined token expiry.

40. The system of claim 39 further comprising a means for allowing the user to conduct a session with the first web server.

41. The system of claim 40 wherein the second web server shares a sub-domain with the first web server.

42. The system of claim 41 wherein the means for digitally signing the authentication token by the first web server comprising means for digitally signing the authentication token using public key encryption.

43. The system of claim 42 further comprising a means for confirming a match with the digital signature.

44. A system of single sign-on for multiple web servers, comprising:

a means for receiving log-in data from a user in a first server;

a means for providing the user with a service selector;

a means for receiving an indication that the user selected the service selector;

a means for constructing an authentication token comprising profile data associated with the user;

a means for encrypting and signing the authentication token;

a means for redirecting the user to a second server;

a means for transmitting the authentication token to the user;

a means for receiving the authentication token in the second server;

a means for verifying the authentication token in the second server; and

a means for allowing the user access to a service provided by the second server.

45. The system of claim 44 wherein the authentication token further comprises expiration time data.

EP 1 089 516 A2

46. The system of claim 45 wherein the authentication token comprises a cookie.

47. The system of claim 46 wherein the log-in data comprises a user name and password.

5 48. The system of claim 47 wherein the service selector comprises a hyperlink.

10

15

20

25

30

35

40

45

50

55

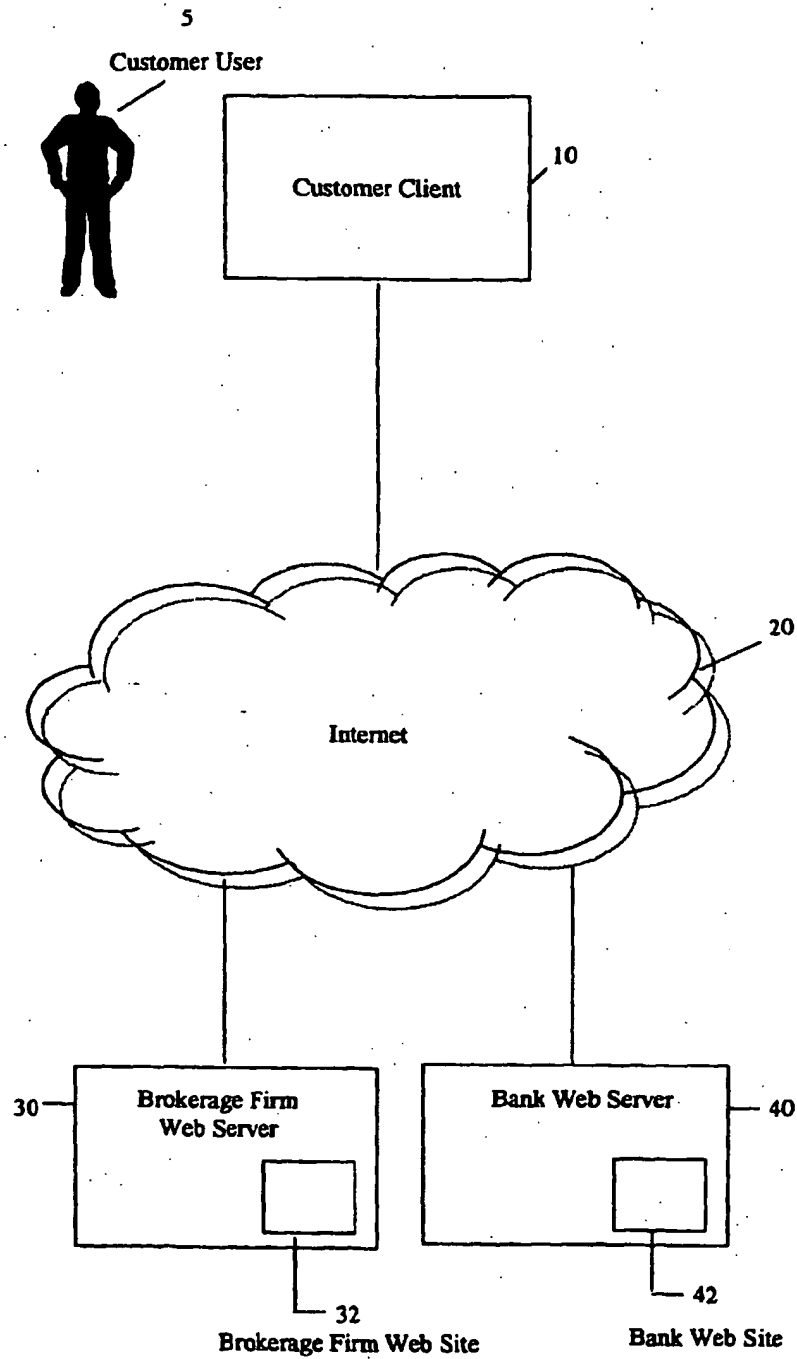


FIG. 1

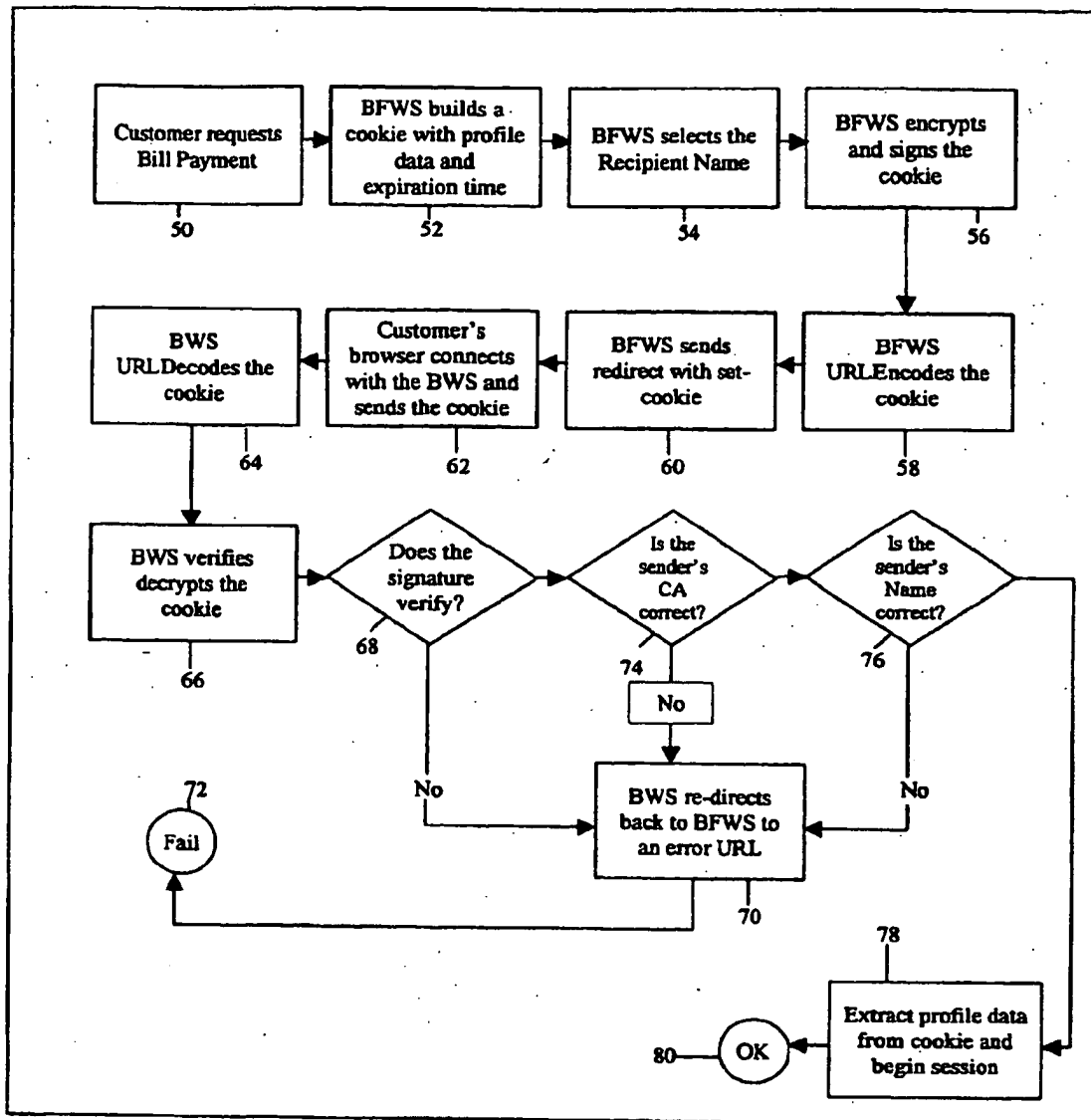


FIG. 2

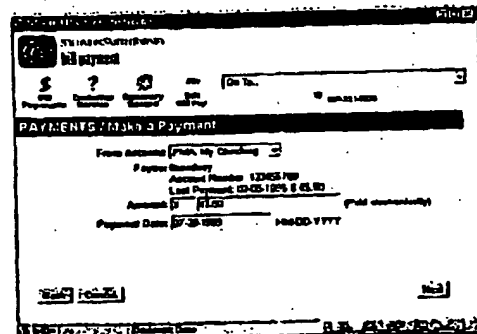
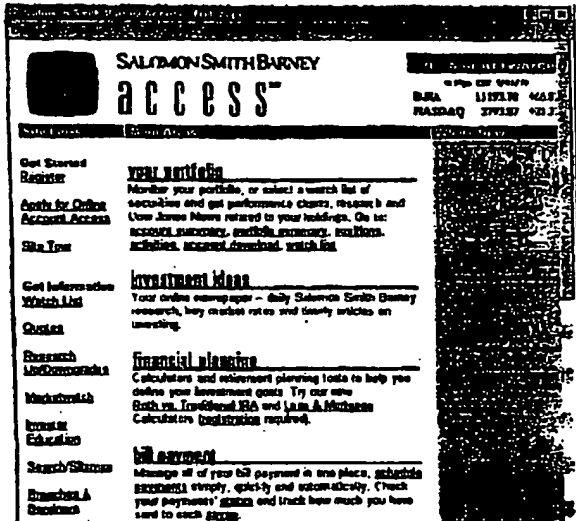
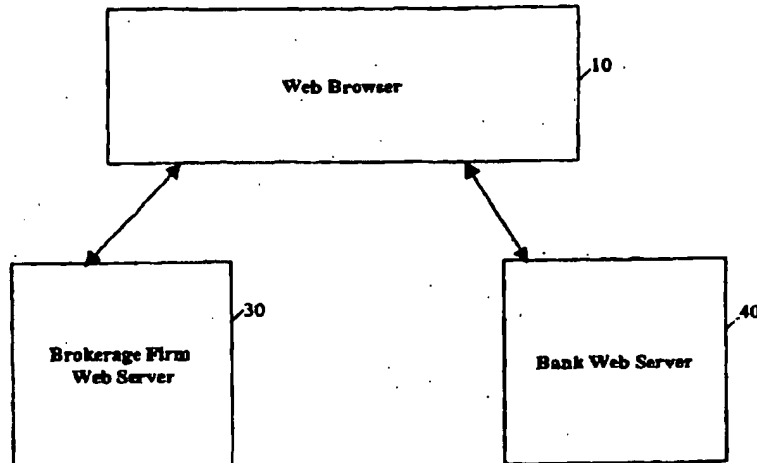


FIG. 3

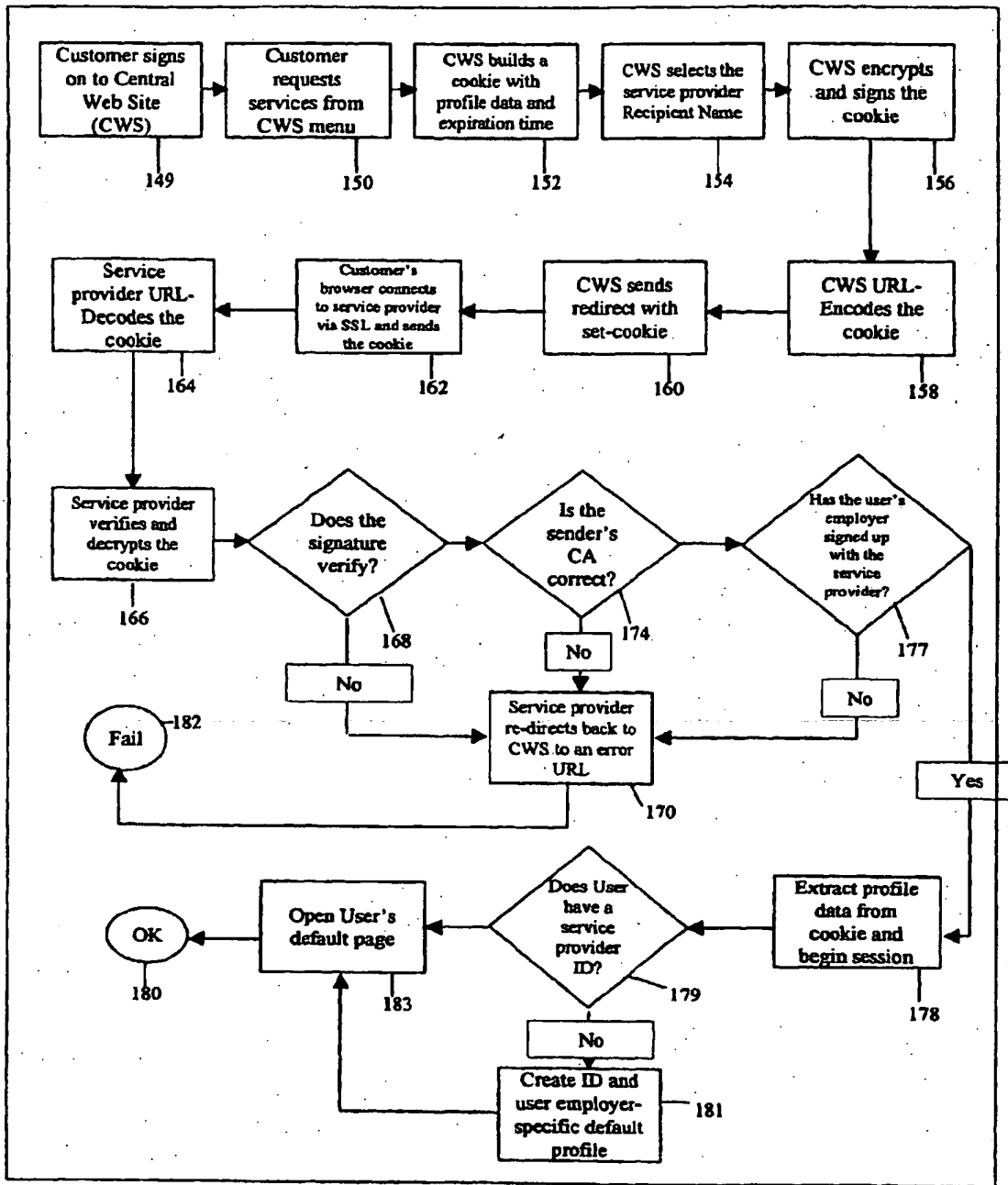
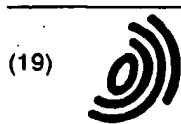


FIG. 4



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 089 516 A3**

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
28.08.2002 Bulletin 2002/35

(51) Int Cl.7: **H04L 29/06, G06F 1/00**

(43) Date of publication A2:
04.04.2001 Bulletin 2001/14

(21) Application number: 00203266.2

(22) Date of filing: 20.09.2000

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 24.09.1999 US 155853 P

(71) Applicant: Citicorp Development Center, Inc.
Los Angeles, California 90066 (US)

(72) Inventors:
• Grandcolas, Michael L.
Santa Monica, CA 90405 (US)
• Law, France
Los Angeles, CA 90034 (US)

- Doshi, Ashwin
Cerritos, CA 90703 (US)
- Williams, Michael
Thousand Oaks, CA 91362 (US)
- Jang, Yeona
Princeton, NJ 08540 (US)
- Merschen, Toni
White Plains, NY 10605 (US)
- Pan, Jack
Rowland Heights, CA 91748 (US)

(74) Representative: Hynell, Magnus
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) Method and system for single sign-on user access to multiple web servers

(57) Methods and systems for single sign-on user access to multiple web servers are provided. A user is authenticated at a first web server (e.g., by user name and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a second web server offering the service indicated by the selector). When the user activates the service selector, the first web server constructs and transmits an encrypted authentication

token (e.g., a cookie) from the first web server to a second web server via the user client. The first and second web servers share a sub-domain. The authentication token comprises an expiration time and is digitally signed by the first web server and is authenticated at the second web server. Upon authentication, the second web server allows the user to conduct a session at the second web server.

EP 1 089 516 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 20 3266

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	J. S. PARK: "Secure Attribute services on the Web" 'Online! June 1999 (1999-06), GEORGE MASON UNIVERSITY, FAIRFAX, VIRGINIA XP002190891 Retrieved from the Internet: <URL: http://www.list.gmu.edu/dissert/diss-jean.pdf> 'retrieved on 2002-02-21!	1-9, 15-23, 25-33, 39-47	H04L29/06 G06F1/00
Y	Chapter 4, Figures A.1-A.10,	10-12, 24, 34-36, 48	
Y	ANSELM BAIRD-SMITH (ABAIRO@WWW18.W3.ORG): "Re: URLEncoder, where is the URLDecoder?" INTERNET NEWSGROUP, 'Online! 29 April 1996 (1996-04-29), XP002191148 comp.lang.java Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-02-21! * the whole document *	10-12, 34-36	
Y	EP 0 913 789 A (SUN MICROSYSTEMS INC) 6 May 1999 (1999-05-06) * claims 1,2 *	24, 48	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L
X	JOON S. PARK: "A Secure Cookie Recipe for Electronic Transactions" 1999 U.S.-KOREA CONFERENCE (UKC) ON SCIENCE, TECHNOLOGY, ENTREPRENEURSHIP, AND LEADERSHIP, , 'Online! 12 - 14 August 1999, XP002191149 UCLA, Los Angeles, California Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/park99secu recookie.html> 'retrieved on 2002-02-21! * the whole document *	1-9	
Y		15-33, 39-48	
		-/--	
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 28 June 2002	Examiner Bertolissi, E
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 (02.02.92) (P/0401)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 20 3266

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	WO 99 20060 A (DSC TELECOM LP) 22 April 1999 (1999-04-22) * page 34, line 1 - page 35, line 5 *	15-33, 39-48	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 28 June 2002	Examiner Bertolissi, E
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 (03.02) (P04011)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 20 3266

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-06-2002

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0913789	A	06-05-1999	EP 0913789 A2	06-05-1999
			JP 11265411 A	28-09-1999
WO 9920060	A	22-04-1999	US 6243451 B1	05-06-2001
			AU 9514398 A	03-05-1999
			EP 1020088 A1	19-07-2000
			WO 9920060 A1	22-04-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82